ISSN:0975-9646

Non-Separable Reversible Data Hiding Based on Histogram Shifting and Random Scramble Encryption

Ajay Trivedi
Asst. Prof.,SDAM College
Hoshangabad

Dr.**Pratima Gautam**
Professor,AISECT University,
Bhopal

Vijay Trivedi
Asst.Prof.,LNCT,
Bhopal

Abstract—**The reversible data hiding techniques, which are used to improve the distortion in images. We have proposed a secure RDH method, Based on Histogram Modification and Random Scramble Transform. This Paper consists different phases for embedding of data, encryption of image, and data extraction/image-recovery. In first phase, the owner gets content's histogram by the inverse s-order technique. After that hides the additional data into the image and then encrypts the image with the help of encryption key. At the receiver end the receiver does not have knowledge about the original content of encrypted image associated with additional data. A receiver gets only the contents of the image after decryption according encryption key, and then extract the embedded data and gets the original image and embedded data separately. In the scheme, the data extraction from decryption is non-separable. The proposed technique was tested for different hiding capacity and the consequences showed that it has excellent output quality. In the tests we get the proposed algorithm to support high capacity rate reach up to approx 0.2 bits per pixel and that is form above 1/4 (25%) from the size of the input image cover file at PSNR above 55 dB for the output signal.**

***Index Terms*— Cover Image, PSNR, Histogram Modification, Reversible Data Hinding (RDH) , Random Scramble, Stego image.**

I. INTRODUCTION

Data hiding is a technique in which data hides into an original (cover) media. The data may be any text like authentication data or author message. At the receiver end hidden data must be extracted. In some high-accuracy applications, it is highly desired that the cover image should be perfectly recovered after data extraction, such as in medical, military and remote sensing. This technique of data hiding fulfill this requirement is called known as reversible data hiding. It is also known as invertible, lossless or distortion free data hiding [1].

Suppose, the owner of the image cannot trust the channel administrator and Data hiding is generally perform by a channel administrator. In such cases, the owner wants to keep the confidentiality of the image. Then he may first encrypt the image using an encryption key and the channel administrator, without knowing content of original image has to hide data into the encrypted image using data hiding key. Receiver can extract the hidden data through data hiding key and recover the original image using encryption key, in a separable mode. The concept of Separable is, if the receiver has only data hiding key than, he will be able to extract the data, but decryption of image is not possible. If he has only encryption key, then he will be able to decrypt the image, but extraction of hidden data is not possible. If the receiver is having both keys, than he will be able to extract the hidden data and recover the cover image [2].

Most of the data hiding techniques are not reversible. Reversible data hiding can be used in different ways like, Integer-to-Integer Wavelet Transform, Difference expansion, and Histogram modification. There are a number of methods which performs data hiding and encryption both.

The main objective of this paper is to implement a Reversible Data Hiding (RDH) method based on Histogram shifting (HS) which gives us high embedding capacity with lowest distortion. Firstly a content owner takes the inverse s-order of the histogram. After that hides the additional data into the image and then encrypts the image using encryption key however the receiver does not have knowledge about the original content of encrypted image associated with additional data. After the decryption a receiver get only the contents of the image according to the encryption key, and then embedded data is extracted and recover the original image and embedded data separately. In the scheme, from the decryption, the data extraction is Non-separable.

The association of the paper is as follows. In the next section II describe basic difference between separable and non-separable RDH. Section III explains the proposed technique , section IV is block diagram of proposed methodology, in section V we define objective visual quality measurements to simulate human perception model, in Section VI gives the results of proposed technique in the form of PSNR, NPCR and Embedding rate using cover image and recovered image, in Section VII future research are discussed.

II. SEPARABLE V/S NON-SEPARABLE REVERSIBLE DATA H IDING

A. *Separable Reversible Data Hiding*

Separable means to divide into different parts, in other words we can divide something in different parts. Here the concept of separable reversible data hiding is that we encrypt the cover image by using of encryption key and the extraction of the payload by using of data hiding key. Both the parts are separated. It means if we have data hiding key than we can extract the hidden data but cannot recover the original image and if we have the encryption key then we can recover the original image but cannot extract the hidden data. We required both of the keys to get the complete received data.

B. *Non-Separable Reversible Data Hiding*

One more technique of reversible data hiding is non-separable Reversible Data hiding. In this technique, the content owner hides the additional data into the image and encrypts the image by the encryption key then transfers it. Here the main aspect of Non-Separable Reversible Data hiding is different from Separable Reversible Data hiding. At the receiver point to extract the original data after performing decryption of the image, we get both separately hiding data and cover image, here we need only one key that is encryption key.

III. PROPOSED METHODOLOGY

We suggest a specialized non-separable reversible data hiding into the image. There are four phases to explain proposed method:

- Data Embedding Phase
- Image Encryption Phase
- Image Decryption Phase
- Data Extraction Phase

The owner of content embeds the top secret data into the image than encrypt the whole image using encryption key. After receiving encrypted image, receiver decrypts image using the encryption key and extracts the data to recover original image. Section A and D describes Data hiding technique along with data extraction and image recovery respectively and Encryption and decryption technique is described in B and C respectively.

.

A. *Data Embedding Phase*

It is a first process of embedding. Initially we Input a gray scale image X with L bits per pixel. From both side Shift the histogram by 1 unit.

Search whole image in an inverse s-order. Compute the pixel difference between the neighboring pixels by the formula,

$$d_i = \begin{cases} x_{i,} & if \;\; i = 0 \\ \left| x_{i-1} - x_i \right| & otherwise \end{cases}$$

Calculate the peak point P from the pixel differences.

By this formula to get stego image Y, where y_i show the stego value of pixel i .If d_i= P, adjust x_i according to the message bit

$$d_i = \begin{cases} x_i + b, if \;\; d_i = p \;\; and \;\; x_i \geq x_{i-1} \\ x_i - b, if \;\; d_i = p \;\; and \;\; x_i < x_{i-1} \end{cases}$$

Where b= message bit to be hide. After modifying the pixel value of original image X we get image Y that is a stego image and it is ready of encryption.

B. *Image Encryption*

Image Encryption process of a given image is divided in to the following steps.

[1]. Firstly we select a stego image Y of M×N pixel size with L bit per pixel .

[2]. Second step of proposed image encryption method based on decomposition of the input stego image Y into bit plane. Since every pixel is form by L bits plane. So when we decompose it, we can get L bit plane image which is described by Y (l) .where l=0, 1….L-1.Decomposition of image Y into lth bit plane is computed by the formula expressed as below.

$$Y^{(l)} = B^{(l)}\left(Y\right)$$

If Y (m, n) is a pixel located at (m, n), then the lth bit of Y(m,n) is:

$$Y^{(l)}\left(m,n\right) = B^{(l)} = \begin{cases} 1 \; if \left(y\left(m,n\right) / 2^{(l)} \right) \bmod 2 = 1 \\ \quad 0 \qquad\qquad\qquad otherwise \end{cases}$$

Next step is to applying Random Scrambling on every bit plane of decomposed image. First we transform the bit plane image Y(l) into a 1-D vector V(l).Then we uses a random natural number generator to produce random sequence R_S and R_D .it takes two different seeds to generate R_S and R_D .The length of R_S and R_D as same length of the rule of bit plane Scrambling given as.

$$V\left(R_S\left(i\right)\right) \leftrightarrow V\left(R_D\left(i\right)\right) i = 0,1,...,\left(M \times N - 1\right)$$

[3]. Once the Scrambling has been done for every bit plane .we merge the scrambled bit planes image to create a transform image Y_T (Scrambled). Next step it's to reconstruct the scrambled bit plane image according to their original level on bit plane. The Reconstruction of Scrambled image is done by the following formula.

$$Y_T = \sum_{l=0}^{L-1} B^{-1(l)}\left(Y^{(l)}\right)$$

[4]. For a pixel at position (m,n) ,we also have.

$$Z\left(m,n\right) = \sum_{l=0}^{L-1} 2^{(l)} \times X^{(l)}\left(m,n\right)$$

After applying these steps we get the final encrypted image.

C. *Image Decryption*

A Reverse process of encrypted image is called as image decryption. Decryption is also systematic or step-by-step procedure to convert encrypted image into original image.

The decryption process is divided into different steps.

[1]. The input is a gray scale encrypted image Z of M×N pixel size with L bit per pixel.

[2]. Bit plane decomposition of the Decrypted image Z into l^th bit plane is computed using the formula described as.

$$Z^{(l)}\left(m,n\right) = B^{(l)} = \left\{\begin{array}{ll} 1 if \left(z\left(m,n\right)/2^{(l)}\right) \bmod 2 = 1 \\ 0 & otherwise \end{array}\right\}$$

We then transform the bit-plane image Z(l) into a 1-D vector V(l) .

[3]. The Next step is to applying anti scrambling on every bit plane image of decrypted image Z. we use again random natural number generator and use the same a couple of seeds used at encryption time to produce same random sequences R_S and R_D with the same length as V and Antiscrambles the 1-D vector V as given formula.

$$V^{(l)}\left(R_S\left(i\right)\right) \leftrightarrow V^{(l)}\left(R_D\left(i\right)\right) i = 0,1,....\left(M \times N - 1\right); l = 0,1,....L-1$$

When the anti-scrambling has been done, final step is to merge the antisrambled bit-plane images according to their original levels on bit-planes and gained an decryptd stego image Y.

D. *Data Extraction*

In this phase receiver extracts the data from decrypted image Y. It is done from the decrypted stego image by searching the image according same order as in the embedding. The message bit b can be extracted by

$$b = \begin{cases} 0, & if \left|y_i - x_{i-1}\right| = P \\ 1, & if \left|y_i - x_{i-1}\right| = P + 1 \end{cases}$$

Where x_{i-1} represent the restored value of y_{i-1}. The original pixel value of x_i determines by:

$$x_i = \begin{cases} y_i, & if \ \left|y_i - x_{i-1}\right| > P \ and \ y_i < x_{i-1}, \\ y_i + 1 & if \ \left|y_i - x_{i-1}\right| > P \ and \ y_i > x_{i-1} \\ y_i - 1, & otherwise \end{cases}$$

If a value 1 is assigned in the location i, restore x_i to its original state by shifting it by 1 unit; otherwise, no need for shifting .

IV. Proposed Block Diagram

The Block diagram of embedding process is divided into the individual blocks such as Inverse S-order, Histogram Calculation, Histogram Shifting, Message Embedding, Message encryption, and Random Scramble Transform as shown in Figure 1.

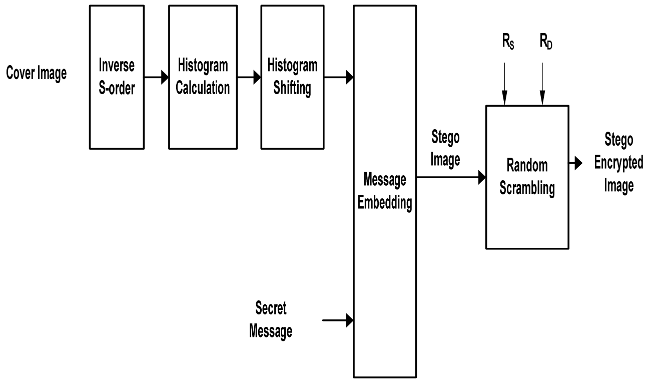


Fig 1: Block diagram of the Proposed Data Hiding Scheme

Figure 2 represents the block diagram of Data Extraction, here encrypted stego image associated with hidden data as a input and output is the recovered hidden data from the input stego image.

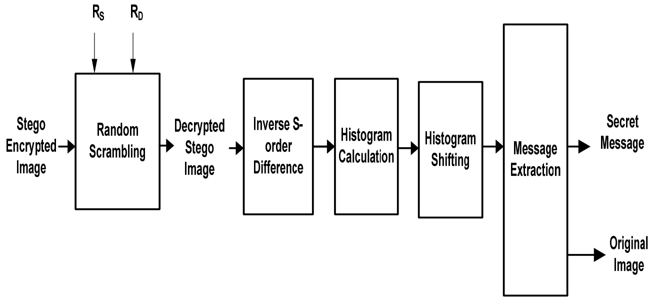


Fig2: Block diagram of the Data Extraction

V. Quality Measurement

The quality of the encrypted image associated with hidden data is measured by calculation of certain evaluation measurement tools. These tools give the evaluation ratio of the original image and the modified image. The quality can be measured depend on these values. The tools used in this paper are as follows: MSE (Mean Square error), PSNR (peak signal- to-noise ratio), NPCR (Number of Pixel Change Rate), CC (Correlation Coefficient) and embedding ratio in BPP.

A. *MSE (Mean square error)*

MSE is quality measurement technique which is frequently used followed by PSNR. The MSE is a average of the squares of intensities difference of the Encrypted image and the cover image. It is represented as:

$$\boxed{MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (C(i,j) - C'(i,j))^2}$$

Where C(i, j) is the original image and C'(i, j) is the encrypted image. If the value of MSE is large that shows the poor quality of image.

B. *PSNR (Peak signal to noise ratio)*

The PSNR refer to measure the quality of restoration of the encrypted image. This tool is used to distinguish quality of cover image and encrypted image. The easy calculation is the advantage of this measure. It is formulated as:

$$\boxed{PSNR = 20 \log 255^2 / MSE}$$

If the value of PSNR is low that shows the constructed image is of poor quality.

C. NPCR (Number of Pixel Change Rate)

NPCR shows the rate of modified pixel of the cover image to get encrypted image. To test the manipulation of a pixel convert the whole encrypted image by the proposed algorithm:

Number of Pixel Change Rate (NPCR)

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

Where:-

D(i, j): Calculated by C1(i, j) and C2(i, j), if C1(i, j) = C2(i,j), then, D(i, j) = 1; otherwise, D(i, j) = 0.

W and H: columns and rows of the image.

C1: Cover image.

C2: Encrypted image.

C1(i, j) and C2(i, j): grey-scale values of the pixels.

D. CC (The Correlation Coefficient)

It is used to measure the encryption quality of any image, stegosystem is the correlation coefficient between the cipher images and pixels at the same indices in the plain. This tool can be calculated by the formula as follows:

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

Where:

x and y are the value of gray-scale pixels at the same indices in the plain and cipher images.

$$E(x) = \frac{1}{L}\sum_{l=1}^{L} X_l \ , \quad E(y) = \frac{1}{L}\sum_{l=1}^{L} Y_l$$

$$D(x) = \frac{1}{L}\sum_{l=1}^{L} \left(x_l - E(x)\right)^2 \ , \quad D(y) = \frac{1}{L}\sum_{l=1}^{L} \left(y_l - E(y)\right)^2$$

$$\operatorname{cov}(x,y) = \frac{1}{L}\sum_{l=1}^{L} \left(x_1 - E(x)\right)\left(y_1 - E(y)\right)$$

E. Bit rate/Embedding Ratio

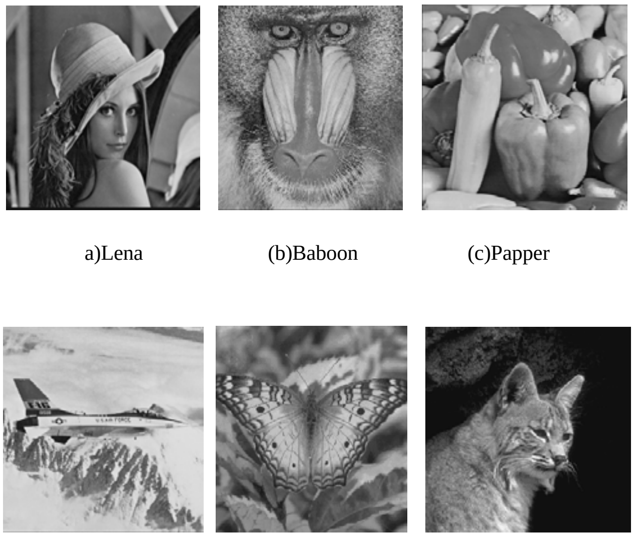
Embedding Ration (Bit rate) represents the amount of bits/pixel hided into the image and it is calculated by formula given below:

$$Bitrate = \frac{Embedding\ Capacity}{Total\ number\ of\ pixels}(bits\ per\ pixel).$$

$$Embedding\ Capacity\ = Total\ number\ of\ pixel.$$

VI. Experiment Result

Proposed technique, was performed on Windows PC having Intel 2.4 GHz processor and 4GB RAM, and run using Matlab 9. The tests were performed with gray scale testing images like Lena and other cover image shown in Figure 3. All the images are 8 bit gray scale images and 256×256 pixels dimension. The embedded data is a text file of size (2048B).



a)Lena (b)Baboon (c)Papper

(d)Plane (e)Butterfly (f)Cat

Fig 3:Test Images of size 256×256

A. Quality Parameter Calculation

The Average of quality parameters between the consequent pixels values of the eight encrypted images Lena, Baboon, Pepper, Boat, Man, Plane, Butterfly and Fish are tabulated in Table 1.

TABLE I QUALITY PARAMETER CALCULATION OF PROPOSED METHOD ON DIFFERENT IMAGES.

Parameter Image	PSNR (53.5225)	Embedded Ratio(BPP) (0.1635)	NPCR (98.9531)	CC (0.0040)
Lena	53.9018	0.09433	99.4781	0.00313
Baboon	50.8396	0.04606	99.3149	0.00412
Pepper	55.554	0.1952	99.3423	0.00422
Boat	56.8612	0.16156	98.9700	0.00486
Man	53.1847	0.08615	99.0961	0.00378
Plane	54.9735	0.19797	98.4222	0.00402
Butterfly	52.8077	0.26591	99.7427	0.00387
Fish	50.0582	0.26033	97.2591	0.00410

We know that higher the values of PSNR show the better quality of the stego image. If PSNR greater than 30 dBs is considered to be an acceptable quality of stego image, and from the table it is clear that PSNR of proposed method is greater then 30 dB (Avg. 53.5225) so we can say that the proposed method gives better stego image quality. Fig. 4 shows the PSNR graph of proposed method on different images.

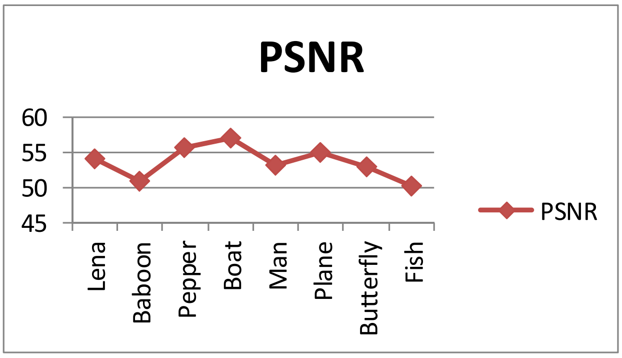


Fig 4: Show PSNR Calculation of proposed method on different images.

Since higher the values of NPCR, it show the better quality of the encrypted image. NPCR grater then 95% is considered to be a better quality encrypted image, and from the table it is clear that NPCR of proposed method is high and gives the better encrypted image quality. Fig. 5 shows the NPCR graph of proposed method on different images.

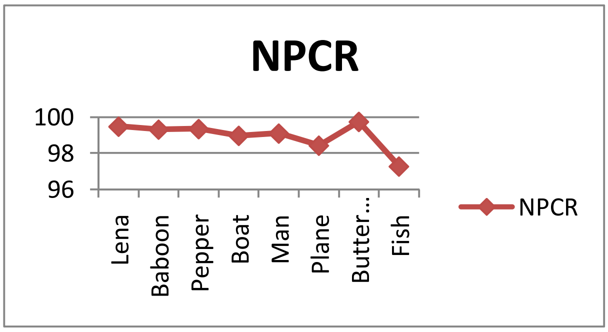


Fig **5: Shows NPCR Calculation of proposed method on different images.**

If the value of Correlation coefficient is greater or equals to one, that means the original image and its encrypted image is identical. And if the value of correlation coefficient equals to zero or less than one that means both encrypted image and original image are completely different that shows good encryption. In the Table 1 there are correlation coefficients of corresponding pixels of the eight encrypted images, where correlation coefficients are worse (Approx 0.0040) .So we can see that in all cases, the plain image is uncorrelated with the cipher image. Fig 6 shows the CC graph of proposed method on different images.

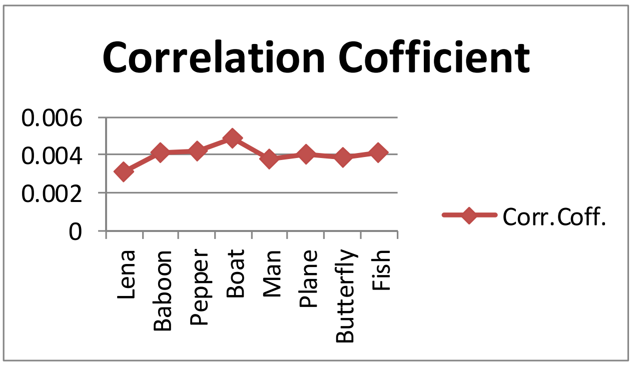


Fig 6: Show CC Calculation of proposed method on different images.

B. Comparative Analysis

We experimented 20 times on the plain Lena's image, in every experiment randomly generated the secret key, and then calculated the PSNR and Embedding Ratio in Stego images. The average value of PSNR and Embedding Ratio are tabulated in Table II. TableII shows that PSNR are better than obtained using the other considered methods. In proposed method, if the image having highest correlation in between adjacent pixels will have the highest embedding capacity and if the image with lower correlation in between pixel have lower embedding capacity. From Tables II that the plain image is highly correlated in diagonal, vertical and horizontal directions, so here embedding ratio is higher compare to other methods. Figure 7 and Figure 8 shows the comparison graph of proposed method with other considered method with respect to PSNR and Embedding Rate respectively.

TABLE II COMPARATIVE ANALYSIS OF PROPOSED DATA HIDING TECHNIQUE

Methods	PSNR	Embedding Rate
W. Tai et.al. [10]	48.3245	0.05545
V. Suresh et.al. [13]	54.1733	0.00497
R Jose et.al. [14]	52.9996	0.01731
G.Coatrieux et.al. [12]	55.7200	0.08123
Proposed Method	56.4564	0.09433

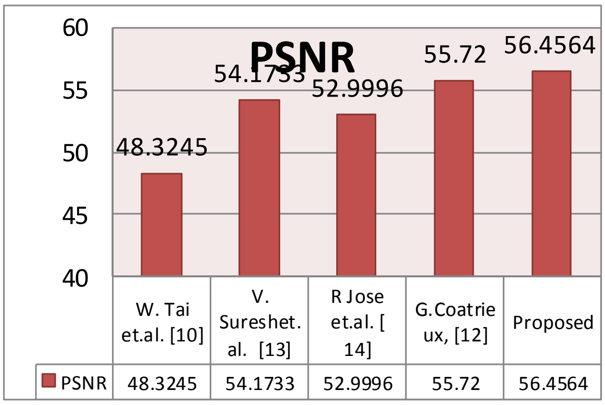


Fig 7 Average PSNR comparison with different image RDH Methods.

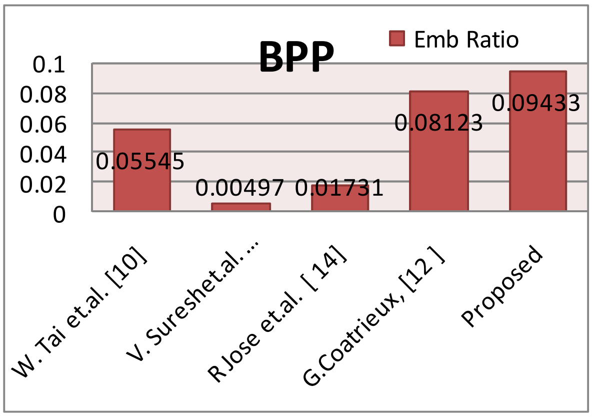


Fig 8 Shows average Correlation between pixel values and compare different RDH Methods.

VII. CONCLUSION

The aim of this research is to enhance the RDH capacity and improve the quality of stego images Here in this paper, we proposed a secure RDH method Based on Histogram Modification and Random Scramble Transform, Which consists of data embedding, image encryption and data extraction/image-recovery phases. In this paper, the data extraction is non-separable from the decrypted image.

The proposed method was tested for different hiding capacity and the final results has excellent output quality. While testing we find the proposed algorithm support high capacity rate reached up to 0.2 approx bits per pixel which is 25% above from the size of the input image cover file at PSNR above 55 dB for the output signal.

The proposed method still need to record extra information for restoring the cover image, in the future the wasting capacity of extra information can reduce.

In future this method can be used for video sequence by separating the video sequences into individual frames.

.

REFERENCES

[1] Zaidoon Kh., AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi," Overview: Main Fundamentals for Steganography ", journal of computing, volume 2, issue 3, March 2010.

[2] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[3] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding-new paradigm in digital watermarking," Eur. Assoc. Signal Process. J. Appl. Signal Process., vol. 2002, no. 2, pp. 185–196, Feb. 2002.

D. Zou, Y. Q. Shi, Z. Ni, and W. Su, "A semi-fragile lossless digital watermarking scheme based on integer wavelet transform," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 10, pp. 1294–1300,Oct. 2006.

[4] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Trans. Inf. Forensic Secur., vol. 2, no. 3, pp. 321–330, Sep. 2007.

[5] J. Tian, "Reversible data embedding using a difference expansion," IEEETrans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[6] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," IEEE Trans. Image Process., vol. 13,no. 8, pp. 1147–1156, Aug. 2004.

[7] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, "A novel difference expansion transform for reversible data embedding," IEEE Trans. Inf. Forensic Secur., vol. 3, no. 3, pp. 456–465, Sep. 2008.

[8] M. Fallahpour and M. H. Sedaaghi, "High capacity lossless data hiding based on histogram modification," IEICE Electron. Exp., vol. 4, no. 7, pp. 205–210, Apr. 2007.

[9] C. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," Pattern Recognit., vol. 41, pp. 3582–3591, 2008.

[10] Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang," Reversible Data Hiding Based on Histogram Modification of Pixel Differences", Ieee Transactions On Circuits And Systems For Video Technology, Vol. 19, no. 6, June 2009.

[11] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, pp. 1129–1143, 2009.

[12] Gouenou Coatrieux, Wei Pan, Nora Cuppens-Boulahia," Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Shifting", IEEE Transactions On Information Forensics And Security, Vol. 8, no. 1, january 2013.

[13] V. Suresh, C. Saraswathy," Separable Reversible Data Hiding Using Rc4 Algorithm" IEEE International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 2013.

[14] Rintu Jose, Gincy Abraham," Separable Reversible Data Hiding in Encrypted Image with Improved Performance", IEEE International Conference on Microelectronics, Communication and Renewable Energy,2013.